

LATHAM & WATKINS LLP
 Elizabeth L. Deeley (CA Bar No. 230798)
elizabeth.deeley@lw.com
 Nicole C. Valco (CA Bar No. 258606)
nicole.valco@lw.com
 505 Montgomery Street, Suite 2000
 San Francisco, CA 94111-6538
 Telephone: +1.415.391.0600
 Facsimile: +1.415.395.8095

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
 555 Eleventh Street, N.W., Suite 1000
 Washington, D.C. 20004-1304
 Telephone: +1.202.637.2200
 Facsimile: +1.202.637.2201

Hilary H. Mattis (CA Bar No. 271498)
hilary.mattis@law.com
 140 Scott Drive
 Menlo Park, CA 94025-1008
 Telephone: +1.650.328.4600
 Facsimile: +1.650.463.2600

*Attorneys for Defendant
 Facebook Inc.*

Andrew N. Friedman (*pro hac vice*)
 Geoffrey Graber (SBN 211547)
 Julia Horwitz (*pro hac vice*)
**COHEN MILSTEIN SELLERS & TOLL
 PLLC**
 1100 New York Ave. NW, Fifth Floor
 Washington, DC 20005
 Telephone: (202) 408-4600
 Facsimile: (202) 408-4699
afriedman@cohenmilstein.com
ggraber@cohenmilstein.com
jhorwitz@cohenmilstein.com

Eric Kafka (*pro hac vice*)
**COHEN MILSTEIN SELLERS & TOLL
 PLLC**
 88 Pine Street, 14th Floor
 New York, NY 10005
 Telephone: (212) 838-7797
 Facsimile: (212) 838-7745
ekafka@cohenmilstein.com

Counsel for Plaintiffs and Proposed Class

**UNITED STATES DISTRICT COURT FOR THE
 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION**

DANIELLE A. SINGER, PROJECT
 THERAPY, LLC (d/b/a THERAPY
 THREADS), HOLLY DEAN, and DZ
 RESERVE, individually and on behalf of all
 others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

Case No.: 3:18-cv-04978-JD

**STIPULATED ~~PROPOSED~~ ORDER
 REGARDING DISCOVERY OF
 ELECTRONICALLY STORED
 INFORMATION**

1 **1. PURPOSE**

2 This Order will govern discovery of electronically stored information (“ESI”) in this case
3 as a supplement to the Federal Rules of Civil Procedure, this Court’s Guidelines for the Discovery
4 of Electronically Stored Information, and any other applicable orders and rules.

5 **2. DEFINITIONS**

6 **A. “Electronically stored information”** or “ESI,” as used herein, has the same
7 meaning as contemplated by the Federal Rules of Civil Procedure.

8 **B. “Metadata”** means and refers to information about information or data about data,
9 and includes without limitation (i) information embedded in or associated with a native file that is
10 not ordinarily viewable or printable from the application that generated, edited, or modified such
11 native file which describes the characteristics, origins, usage and/or validity of the electronic file
12 and/or (ii) information generated automatically by the operation of a computer or other information
13 technology system when a native file is created, modified, transmitted, deleted or otherwise
14 manipulated by a user of such system.

15 **C. “Documents”** has the meaning contemplated in the Federal Rules of Civil
16 Procedure.

17 **D. “Media”** means an object or device, real or virtualized, including but not limited
18 to a disc, tape, computer or other device, on which data is or was stored.

19 **3. COOPERATION**

20 The parties are aware of the importance the Court places on cooperation and commit to
21 cooperate in good faith throughout the matter consistent with this Court’s Guidelines for the
22 Discovery of ESI.

23 **4. LIAISON**

24 The parties have designated e-discovery liaison(s) to each other who are and will be
25 knowledgeable about and responsible for discussing their respective ESI and the party’s discovery
26 efforts. Each e-discovery liaison will be, or have access to those who are, familiar with the party’s
27 electronic systems and capabilities in order to explain those systems and answer relevant questions.
28 Each e-discovery liaison will be, or have reasonable access to those who are, knowledgeable about

the technical aspects of e-discovery, including electronic document storage, organization, and format issues, and the location, nature, accessibility, format, collection, search methodologies, and production of ESI in this matter. The parties will rely on the liaisons, as needed, to confer about ESI and to help resolve disputes without court intervention where possible.

5. PRESERVATION

Each party is responsible for taking reasonable and proportionate steps to preserve relevant and discoverable ESI within its possession, custody or control. The parties have discussed their preservation obligations and needs and agree that preservation of potentially relevant ESI will be reasonable and proportionate. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

(a) The parties shall preserve non-duplicative discoverable information currently in their possession, custody or control, however, parties shall not be required to modify, on a going-forward basis, the procedures used by them in the usual course of business to back up and archive data.

(b) Only ESI created or received after January 1, 2013, through the close of fact discovery on December 13, 2019 will be preserved;

(c) The parties will discuss the types of ESI they believe should be preserved and the custodians, or general job titles or descriptions of custodians, for whom they believe ESI should be preserved, *e.g.*, “HR head,” “scientist,” and “marketing manager.” The parties shall add or remove custodians as reasonably necessary;

(d) The parties will agree on the number of custodians per party for whom ESI will be preserved;

(e) These data sources are not reasonably accessible because of undue burden or cost pursuant to Fed. R. Civ. P. 26(b)(2)(B) and ESI from these sources will be preserved pursuant to normal business retention, but not searched, reviewed, or produced, unless otherwise ordered by the Court upon a motion of a party:

1. backup systems and/or tapes used for disaster recovery; and
2. systems that are no longer in use and cannot be accessed.

1 (f) Among the sources of data the parties agree are not reasonably accessible, based on
2 mutual representation of the parties' counsel, the parties agree not to preserve, collect,
3 process, review and/or produce the following:

- 4 1. Deleted, slack, fragmented, or unallocated data only accessible by forensics;
- 5 2. Random access memory (RAM), temporary files, or other ephemeral data
6 that are difficult to preserve without disabling the operating system;
- 7 3. On-line data from the employees of the producing party using internet
8 browsers, such as temporary internet files, history, cache, cookies, and the
9 like;
- 10 4. Data in the following metadata fields that are frequently updated
11 automatically: last opened dates and times, last modified dates and times,
12 last printed dates and times, and last modified by (except the parties must
13 produce if available the last date modified and last modified time as required
14 by Appendix 1);
- 15 5. Voice messages. The parties will preserve only those voice messages that
16 a custodian identifies may have potentially relevant information. (To avoid
17 any doubt, voice messages will also be preserved if they attached to an e-
18 mail family that is being preserved);
- 19 6. Sound recordings, including, without limitation, .mp3 and .wav files. The
20 parties will preserve only those sound recordings that a custodian identifies
21 may have potentially relevant information. (To avoid any doubt, sound
22 recordings will also be preserved if they are attached to an e-mail family
23 that is being preserved.);
- 24 7. Information contained on mobile devices. The parties will preserve only
25 that information contained on a mobile device that a custodian identifies
26 may have potentially relevant information and which is not duplicative of
27 information that resides in a reasonably accessible data source;
- 28 8. Mobile device activity logs for the producing party's employees;

9. Information created or copied during the routine, good-faith performance of processes for the deployment, maintenance, retirement, and/or disposition of computer equipment by the party and belonging to a custodian, to the extent such information is duplicative of information that resides in a reasonably accessible data source; and

10. Other forms of ESI whose preservation requires unreasonable and/or disproportionate affirmative measures that are not utilized in the ordinary course of business.

6. SEARCH AND REVIEW

A. Cooperation on Scope. The parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery.

B. Cooperation on Search Terms. The parties understand the cost and complexity of reviewing and producing ESI and seek to engage in a cooperative, iterative process to limit costs but ensure relevant, responsive documents are likely discovered in any ESI search. As such, the parties will cooperate regarding the disclosure and formulation of appropriate search terms for use in the responsiveness review and production of ESI. The parties are not required to exchange privilege search terms.

C. Disclosure of Records Custodians. The parties will each disclose a list of the most likely custodians of relevant documents, including the general job titles or descriptions of each custodian and information relating to the type of relevant documents that each custodian is expected to possess, and/or ESI.

D. Search Terms and Custodians.

1. Whether or not the parties opt to use Technology-Assisted Review (“TAR”), the producing party—with greater familiarity of the terminology used by its client(s)—will first provide search terms and likely custodians of ESI.

2. The parties will meet-and-confer in good faith regarding search terms and

1 custodians.

2 3. As part of the meet-and-confer process to select search terms and custodians, the
3 producing party must provide a hit report if reasonably requested by the receiving party.

4 **E. Additional Custodians and Search Terms.**

5 1. Parties may request additional search terms or custodians. Such requests must be
6 made in good faith. The parties will meet and confer on whether an extension of time for fact
7 discovery will be necessary depending on the additional volume of the request.

8 2. Any disputes over additional custodians or terms pursuant to this paragraph shall,
9 after meet and confer, be presented to the Court.

10 3. The parties will continue to meet and confer regarding any search process issues as
11 necessary and appropriate. This ESI protocol does not address or resolve any other objection to the
12 scope of the parties' respective discovery requests.

13 **F. Responsiveness Review**

14 Nothing in this Order shall be construed or interpreted as precluding a producing party
15 from performing a responsiveness review to determine if documents captured by search terms are
16 in fact relevant to the requesting party's request. Further, nothing in this Order shall be construed
17 or interpreted as requiring the production of all documents captured by any search term if that
18 document is in good faith and reasonably deemed not relevant to the requesting party's request or
19 is privileged.¹ The producing party may not redact portions of documents for relevancy without
20 the agreement of the receiving party.

21 **F. Non-Custodial Searches and Non-Search Term Collection**

22 Searches of custodial databases using search terms do not relieve a party of the obligation
23 to (a) search non-custodial databases and (b) collect documents without using search terms. The
24 parties will work cooperatively to identify the types of documents that can and should be collected
25

26 ¹ The producing party will disclose to the receiving party if they intend to use Technology
27 Assisted Review ("TAR") (including predictive coding or any other form of machine learning) to
28 filter out non-responsive documents. If the receiving party objects to the use of TAR (including
predictive coding or any other form of machine learning), then the parties will meet-and-confer.
Any dispute shall be presented to the Court for resolution.

1 from non-custodial repositories. The parties will work cooperatively to identify the types of
2 documents that can and should be collected without using search terms.

3 **7. PRODUCTION FORMATS**

4 The parties agree to produce documents in the formats described in Appendix 1 to this
5 Order. If particular documents warrant a different format, the parties will cooperate to arrange for
6 the mutually acceptable production of such documents. The parties agree not to degrade the
7 searchability of documents as part of the document production process.

8 **8. MISCELLANEOUS PROVISIONS**

9 **A. Duplicates.**

10 The parties have agreed to de-duplicate identical copies of electronic documents (i.e., the
11 documents are exact duplicates based on MD5 hash values at the document level) across their
12 custodians or sources. Where a producing party has more than one identical copy of an electronic
13 document, the producing party need only produce a single copy of that document (as long as all
14 family relationships are maintained). If the document was de-duplicated, the producing party must
15 identify each custodian or source where the document was located in a coding field. For emails
16 with attachments, the hash value is generated based on the parent/child document grouping. To
17 the extent that de-duplication through MD5 hash values is not possible, the parties shall meet and
18 confer to discuss any other proposed method of de-duplication.

19 **B. Email Threading.**

20 Email thread analysis may be used to reduce the volume of e-mails reviewed and produced,
21 provided that the parties disclose such use. Where multiple email messages are part of a single
22 chain or “thread,” a party is only required to produce the most inclusive message (“Last In Time
23 Email”) and need not produce earlier, less inclusive email messages or “thread members” that are
24 not unique and therefore fully contained, including attachments and including identical senders
25 and recipients, within the Last In Time Email. Only email messages for which the parent document
26 and all attachments are contained in the Last In Time Email will be considered less inclusive email
27 messages that need not be produced.
28

C. Non-Substantive Files.

Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library (“NSRL”) NIST Hash Set List. System and program files defined on the NIST list need not be processed, reviewed, or produced. The parties may suppress container files (.ZIP, .PST, .RAR) that do not reflect substantive information prior to production, but must produce the remainder of those responsive, non-privileged document families found within the container file, including any emails to which that container file is attached. Similarly, the parties may suppress any non-substantive images extracted from email documents (e.g., logs, icons) prior to production).

9. DOCUMENTS PROTECTED FROM DISCOVERY

A. Waiver

Pursuant to Fed. R. Evid. 502(d), the production of a privileged or work-product-protected document, whether inadvertent or otherwise, is not a waiver of privilege or protection from discovery in the pending case or in any other federal or state proceeding. Disclosures among defendants’ attorneys of work product or other communications relating to issues of common interest shall not affect or be deemed a waiver of any applicable privilege or protection from disclosure. For example, the mere production of privileged or work-product-protected documents in this case as part of a mass production is not itself a waiver in this case or in any other federal or state proceeding. A producing party may assert privilege or protection over produced documents at any time by notifying the receiving party in writing of the assertion of privilege or protection. Information that contains privileged matter or attorney work product shall be returned immediately or destroyed if such information appears on its face to have been inadvertently produced, or if requested. The receiving party must return or destroy ESI that the producing party claims is privileged or work-product-protected as provided in Rule 26(b)(5)(B) and may use such ESI only to challenge the claim of privilege or protection.

B. Privilege Log Format and Timing.

1. In an effort to avoid unnecessary expense and burden, the parties agree that, for all

1 documents, ESI, or other information that has been redacted or withheld from production on the
2 basis of attorney-client privilege, the work product doctrine, and/or any other applicable privilege,
3 and in connection with the provision of any applicable privilege log required pursuant to Fed. R.
4 Civ. P. 26, the producing party will prepare a privilege log containing document type, the
5 Custodian, Email Author, Email Recipient, Email CC, Email BCC, File Author, and File Created
6 Date, to the extent such information exists and does not disclose privileged information. The
7 producing party's privilege log shall include a description of the nature of the document (or
8 redacted portion thereof), with sufficient specificity that—without revealing information itself
9 privileged—will enable the other parties to assess the privilege claim. The producing party's
10 privilege log shall also include the type of privilege being asserted.

11 2. Redaction Logs. Separate redaction logs will be produced to cover redactions.
12 Because the underlying documents have been produced, redaction logs need include only a unique
13 number, the beginning Bates number of the document, the ending Bates number, a description of
14 what has been redacted, including, where applicable, a description of the type of privilege being
15 asserted and the reason for privilege.

16 3. The privilege log and/or redaction log will be produced in Microsoft Excel.

17 4. Within 30 business days of receiving such a summary log, a receiving party may
18 identify particular documents or redacted information that it asserts is not privileged or that require
19 further explanation. The receiving party shall explain in writing its basis for asserting that such
20 documents or information is not privileged or the need for additional information and state
21 precisely each document (by Bates number or privilege log entry) for which it disputes the
22 privilege designation or seeks additional information. Within 14 days of such a request, or within
23 a reasonable time depending on volume, the producing party must (i) inform the receiving party
24 which documents listed on the privilege log or redaction log (if any) the producing party will
25 produce and (ii) provide any additional information (if any) that the producing party is willing to
26 provide. If the receiving party still asserts that there are documents or information that was
27 improperly designated as privileged, the Parties shall meet and confer to try to reach a mutually
28 agreeable solution. If they cannot agree, the matter shall be brought to the Court.

6. The Parties agree to log only the Last In Time Emails and need not log earlier, less inclusive email messages or “thread members” that are fully contained within the Last In Time Email and therefore were suppressed from review in the first instance.

7. Any written and oral communications between a party and its outside counsel or inside counsel, or between inside and outside counsel, in connection with this Action (after commencement of the Action), and work product material prepared in connection with this Action (after commencement of the Action), do not require a privilege log.

8. Nothing in this Order shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity. The parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of documents and ESI.

11. MODIFICATION

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

DATED: May 23, 2019

LATHAM & WATKINS LLP

/s/ Elizabeth L. Deeley
Elizabeth L. Deeley (Bar No. 230798)
elizabeth.deeley@lw.com
Nicole C. Valco (Bar No. 258506)
nicole.valco@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Telephone: +1.202.637.2200
Facsimile: +1.202.637.2201

Hilary H. Mattis (Bar No. 271498)
hilary.mattis@lw.com
140 Scott Drive
Menlo Park, CA 94025-1008
Telephone: +1.650.328.4600

Facsimile: +1.650.463.2600

Attorneys for Defendant Facebook, Inc.

DATED: May 23, 2019

COHEN MILSTEIN SELLERS & TOLL PLLC

/s/Geoffrey Graber

Andrew N. Friedman (*pro hac vice*)

Geoffrey Graber (Bar No. 211547)

Eric Kafka (*pro hac vice*)

Julia Horwitz (*pro hac vice*)

1100 New York Ave. NW, Fifth Floor

Washington, DC 20005

Telephone: (202) 408-4600

Facsimile: (202) 408-4699

afriedman@cohenmilstein.com

ggraber@cohenmilstein.com

ekafka@cohenmilstein.com

jhorwitz@cohenmilstein.com

Attorneys for Plaintiffs

IT IS ORDERED that the forgoing Agreement is approved.

DATED: June 6, 2019


Judge James Donato

SIGNATURE ATTESTATION

I am the ECF User whose identification and password are being used to file Stipulated [Proposed] Protective Order regarding signatures, I, Elizabeth L. Deeley, attest that concurrence in the filing of this document has been obtained.

DATED: May 23, 2019

/s/ Elizabeth L. Deeley

Elizabeth L. Deeley

APPENDIX 1: PRODUCTION FORMAT

1. **Production Components.** Except as otherwise provided below, ESI shall be produced in accordance with the following specifications:

- (a) an ASCII delimited data file (.DAT) using standard delimiters;
- (b) an image load file (.OPT) that can be loaded into commercially acceptable production software (*e.g.* Concordance);
- (c) TIFF images;
- (d) and document level .TXT files for all documents containing extracted full text or OCR text.

If a particular document warrants a different production format, the parties will cooperate in good faith to arrange for a mutually acceptable production format.

2. **Production Media and Access Controls.** Documents shall be encrypted and produced through electronic means, such as secure file sharing methods (*e.g.* FTP), or on CD, DVD, flash drive or external hard drive (“Production Media”). Each piece of Production Media shall identify a production number corresponding to the production volume (*e.g.* “VOL001”). Each piece of Production Media shall also identify: (a) the producing party’s name; (2) the production date; (3) the Bates Number range of the materials contained on the Production Media.

Nothing in this Order will preclude or impair any and all protections provided the parties by any Protective Order(s) agreed and entered into by the parties. Any data produced by the producing party must be protected in transit, in use, and at rest by all in receipt of such data. Parties will use best efforts to avoid the unnecessary copying or transmittal of produced documents. Any copies made of produced data must be kept on media or hardware employing whole-disk or folder level encryption or otherwise secured on information systems and networks in a manner consistent with the best practices for data protection. The data protection should comply with ISO 27001 or higher and include reasonable

administrative, technical, and physical safeguards designed to protect the security and confidentiality of the produced data, protect against any reasonably anticipated threats or hazards to the security of such produced data, and protect against unauthorized access to or use of such produced data. If questions arise, Parties will meet and confer to ensure security concerns are addressed prior to the exchange of any documents.

3. **Data Load Files/Image Load Files.** Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s) in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. All images must be assigned a unique Bates number that is sequential within a given document and across the production sets. The Bates Numbers in the image load file must match the corresponding documents' beginning Bates numbers in the data load file. The total number of documents in a production should match the total number of records in the data load file. Load files shall not vary in format or structure within a production, or from one production to another.
4. **Metadata Fields.** Each of the metadata and coding fields set forth below that can be extracted shall be produced for each document. The parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document, with the exception of the following: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH, (e) CUSTODIAN, (f) ALLCUSTODIANS, (g) CONFIDENTIALITY, (h) REDACTIONS, (i) NATIVEFILEPATH, (j) TEXTFILEPATH, and (k) MD5HASH, which should be populated by the party or the party's vendor. The parties will make reasonable efforts to ensure that metadata fields automatically extracted from the documents correspond directly to the information that exists in the original documents.

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
CUSTODIAN	Individual from whom the documents originated
ALLCUSTODIANS	Custodians who had copy of document but whose copies were eliminated via deduplication.
CONFIDENTIALITY	Confidentiality designation assigned to document
REDACTIONS	Designation to indicate whether the document contains redactions
HAS HIDDEN DATA	Designation indicating whether document has hidden data.
NATIVEFILEPATH	Native File Link (Native Files only)
DOCEXT	The file extension
TEXTFILEPATH	Path to extracted text/OCR file for document
MD5HASH	MD5 hash value of document
AUTHOR	Any value populated in the Author field of the document properties (Edoc or attachment only)
EMAILSUBJECT	The subject of the email
FILENAME	Any value populated in the Filename field of the document properties
DOCDATE	Date the document was created (format: MM/DD/YYYY) (Edoc or attachment only)
DOC CREATED TIME	The time the document was created (format HH:MM:SS) (Edoc or attachment only)
DATEMODIFIED	Date when document was last modified according to filesystem information (format: MM/DD/YYYY) (Edoc or attachment only)
DATE MODIFIED TIME	The time the document was last modified (format HH:MM:SS) (Edoc or attachment only)
FROM	The name and email address of the sender of the email

Field Name	Field Description
TO	All recipients that were included on the “To” line of the email
CC	All recipients that were included on the “CC” line of the email
BCC	All recipients that were included on the “BCC” line of the email
DATRECEIVED	Date email was received (format: MM/DD/YYYY)
TIMERECEIVED	Time email was received (format: HH:MM:SS)
DATESENT	Date email was sent (format: MM/DD/YYYY)
TIMESENT	Time email was sent (format: HH:MM:SS)
TIME OFFSET VALUE	Indicate which time zone the data is set to when processed.
FILESIZE	The original file size of the produced document
PRODVOL	Production volume.

5. **TIFFs.** Documents that exist only in hard copy format shall be scanned and produced as TIFFs. Documents that exist as ESI shall be converted and produced as TIFFs, except as provided below. The parties shall take reasonable efforts to process presentations (*e.g.* MS PowerPoint) with hidden slides and speaker’s notes unhidden, and to show both the slide and the speaker’s notes on the TIFF image. Unless excepted below, single page, black and white, Group IV TIFFs should be provided, at least 300 dots per inch (dpi) for all documents. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed upon confidentiality designation. Original document orientation should be maintained (*i.e.*, portrait to portrait and landscape to landscape). Where the TIFF image is unreadable or has materially degraded the quality of the original, the producing party shall provide a higher quality TIFF image or the native or original file.
6. **Color.** The parties will produce any Quips in color. The parties may request color copies of a limited number of other documents where color is necessary to accurately interpret the document.

- 1 7. **Text Files.** A single multi-page text file shall be provided for each document, and the
 2 filename should match its respective TIFF filename. When possible, the text of native files
 3 should be extracted directly from the native file. Text files will not contain the redacted
 4 portions of the documents. A commercially acceptable technology for optical character
 5 recognition “OCR” shall be used for all scanned, hard copy documents and for documents
 6 with redactions.
- 7 8. **Native Files.** Microsoft Excel and PowerPoint files will be produced in native format. To
 8 the extent that they are produced in this action, audio, video, and multi-media files will be
 9 produced in native format. Native files shall be produced with a link in the
 10 NATIVEFILEPATH field, along with extracted text (where extracted text is available) and
 11 applicable metadata fields set forth in paragraph 4 above. A Bates numbered TIFF
 12 placeholder indicating that the document was provided in native format must accompany
 13 every native file. The parties agree to work out a protocol for use of native files at
 14 depositions, hearings, or trial.
- 15 (a) The requesting party may request the production of files not specifically listed in
 16 Number 8 above in native format. In making such a request, however, the requesting
 17 party must establish good cause for the request and include a detailed explanation of
 18 the need for native file review. The producing party shall not unreasonably deny the
 19 request if good cause for native production exists.
- 20 9. **Confidentiality Designation.** Responsive documents in TIFF format will be stamped with
 21 the appropriate confidentiality designations in accordance with the protective order entered
 22 in this matter. Each responsive document produced in native format will have its
 23 confidentiality designation identified in the filename of the native file and indicated on its
 24 corresponding TIFF placeholder.
- 25 10. **Databases and Other Structured Data.** The information will be produced in a reasonably
 26 usable form, which may include Microsoft Excel or Microsoft Access. To the extent a party
 27 is constrained from producing responsive ESI because of a third party license or because
 28 software necessary to view the ESI is hardware-dependent, the parties shall meet and

1 confer to reach an agreement on alternative methods to enable the requesting party to view
 2 the ESI. The parties shall meet and confer regarding the production format and scope of
 3 data contained in databases in order to ensure that any information produced is reasonably
 4 usable by the receiving party and that its production does not impose an undue burden on
 5 the producing party. To avoid doubt, information will be considered reasonably usable
 6 when produced in CSV format, tab-delimited text format, Microsoft Excel format, or
 7 Microsoft Access format.

8 11. **Attachments.** Email attachments and embedded files or links must be mapped to their
 9 parent by the Document or Production number. If attachments and embedded files are
 10 combined with their parent documents, “BeginDoc” and “EndDoc” fields listing the unique
 11 beginning and ending number for each document and “BeginAttach” and “EndAttach”
 12 fields listing the begin and end of the entire document family must be included.

13 12. **Embedded Objects.** Objects embedded in Microsoft Word and .RTF documents, which
 14 have been embedded with the “Display as Icon” feature, will be extracted as separate
 15 documents and treated like attachments to the document. Other objects embedded in
 16 documents shall be produced as native files.

17 13. **Compressed Files.** Compression file types (i.e., .CAB, .GZ, .TAR, .Z, .ZIP) shall be
 18 decompressed in a reiterative manner to ensure that a .zip within a .zip is decompressed
 19 into the lowest possible compression resulting in individual folders and/or files.

20 14. **Inaccessible or Unusable ESI.** If a producing party asserts that certain requested ESI is
 21 inaccessible or otherwise unnecessary under the circumstances, or if the receiving party
 22 asserts that, following production, certain ESI is not reasonably usable, the parties shall
 23 meet and confer to discuss resolving such assertions. If the parties cannot resolve any such
 24 disputes after such a meet and confer has taken place, the issue shall be presented to the
 25 Court for resolution.